CHAPTER 4

RISK ASSESSMENTS

0401 GENERAL

040101. Purpose. This chapter provides detailed guidance on National Aeronautics and Space Administration's (NASA) financial management internal control program policies, procedures, and responsibilities within the Agency related to conducting risk assessments, developing Corrective Action Plans (CAP) when needed, and monitoring recommended corrective actions as a result of the assessments. This process supports the internal control process developed by the Office of Quality Assurance (OQA) in compliance with Office of Management and Budget (OMB) Circular A-123 "Management's Responsibility for Internal Control" and Government Accountability Office (GAO) internal control standards.

040102. Risk assessment is the identification and analysis of relevant risks or vulnerabilities associated with achieving an assessable unit's (AU's) mission and objectives. This systematic analysis identifies a program's or function's susceptibility to failing to achieve its objectives or goals; to producing erroneous reports or data; to allowing unauthorized use of resources, or permitting illegal or unethical acts; and to receiving an adverse or unfavorable financial statement audit opinion.

040103. A risk assessment is conducted in order to appropriately identify, measure, and prioritize risks so attention can be placed on those identified areas of greatest risk. It also ensures that proper internal controls are in place to manage identified risks. Risk assessments help assure the Office of the Chief Financial Officer's (OCFO's) organizational internal control structure is well designed and operated, appropriately updated to meet changing conditions, and provide reasonable assurance that NASA and OCFO's objectives are being achieved.

0402 REQUIREMENTS

040201. Responsibility. Risk assessments must be performed for each AU, as defined during the establishment of assessable units (see Volume 9, Chapter 3 for guidance). Each assessment should be fully documented on the "Financial Management Internal Control Risk Assessment Form" (see Appendix 2 for form and form with examples) and should be kept on file at each respective office. The Agency OCFO, Center CFO, Mission Directorates, Mission Support Offices, NASA Competency Center, and the NASA Shared Services Center (NSSC) will be responsible for assuring that its risk assessments are completed for each AU. Responsibility for completing the assessment should be delegated to an AU point of contact.

040202. Risk assessment steps. A risk assessment should consist of the following steps. All steps should be fully documented, per the requirements outlined in this Volume.

A. Describe AU activities

B. Determine objectives (type and category)

C. Identify and prioritize risks

D. Determine control techniques and activities

E. Identify other objectives affected

F. Document/brief conclusion

G. Develop Corrective Action Plan (if necessary)

040204. Describe AU activities. To properly examine the AU's risks, objectives, and control techniques, a stable and concrete point of reference must be defined. The evaluator should provide a brief narrative description of the AU's standard activities. Though not required, a process flow diagram would also assist the evaluator in providing a basis for conducting a structured and logical examination of the organization and activities.

040205. Determine objectives. A precondition to risk assessment is the establishment of clear and consistent objectives. The NASA Administrator and the Chief Financial Officer have developed objectives outlining a "building block" strategy that will enable NASA to accomplish its goals. The OCFO is a key participant in the process through the integration of finance, procurement, and other functions that support the Mission Directorates as they plan for, acquire, and use resources.

The OCFO has developed goals with supporting objectives and measures which are being used to gauge performance. Each objective is supported by multiple initiatives that will be monitored to assess progress against the goals. These goals, objectives, measures, and initiatives provide the blueprint for the OCFO, both Headquarters and Center operations, in guiding day-to-day operations and improving services.

Just as the OCFO goals and objectives are linked to NASA's overall goals and objectives, assessable unit objectives should be linked to the OCFO's goals and objectives. The assessable unit objectives, along with the risks and control techniques and activities, should be specific to the process the assessable unit carries out. By assuring the AU's control techniques and activities are in place and operating effectively, the AU is more likely to achieve its' objectives which in turn is a critical success factor in enabling the OCFO to achieve its' objectives.

The evaluator must document all appropriate objectives associated with each AU activity and identify the objective category (e.g. operations, financial, or compliance).

A. Objective types. There are two primary types of objectives, as defined in the GAO "Standards for Internal Control" – entity-wide and activity-wide. The evaluator will be conducting risk assessments primarily at the activity-level.

1. Entity-wide objectives are high-level and include broad statements of what an entity desires to achieve, and are represented by the mission and vision statements and supported by related strategic plans.

2. Activity-level objectives flow from and are linked with the entity-wide objectives and strategies. Activity-level objectives are at a lower level than entity-wide and are frequently stated as goals with specific targets and deadlines. The activity-level objectives in the organization consists of functions such as procurement, budget, contracts management, and financial.

B. Objective categories. In addition to the types of objectives, certain broad categories of objectives have been established. The evaluator must identify a category for each objective identified in the AU. The categories are defined as operations, financial, or compliance.

1. Operations objectives pertain to effectiveness and efficiency of the organization's operations, including performance goals and safeguarding resources against loss. They vary based on management's choices about structure and performance.

2. Financial reporting objectives pertain to the preparation of supporting documentation necessary to produce reliable and auditable published financial statements. They are driven primarily by external requirements such as the Federal Financial Management Improvement Act of (1996) (FFMIA) and the Federal Accounting Standards Advisory Board (FASAB) accounting standards.

3. Compliance objectives pertain to adherence to laws and regulations to which the organization is subject. They are dependent on external factors, such as public laws, NASA Financial Management Requirements (FMRs), NASA Policy Directives (NPDs), and OMB Circulars.

040206. Identify and prioritize risks. The determination of risks that exist within the AU under review is one of the most important phases of the risk assessment. Control systems are developed in response to risks that exist within the AU. Risks should be developed first, without consideration for controls currently in place to mitigate those risks. Even though the evaluator may believe that controls are in place to adequately address a given risk, the risk should still be identified, prioritized, and examined during the assessment. By doing so, the reviewer is confirming the existence of good management practices within the AU and covering all significant risks in the assessment.

All objective categories have some degree of risk. A statement of risk is related to a negative event or situation that occurs if all or a part of the process under review is not carried out as planned. The risk describes an event or situation the AU does not want to occur. All risks should be identified, even if the AU does not have control over the risk. The evaluator should consider the impact of each risk.

A. Risk factors. Various factors should be considered when identifying risks. Each of the factors listed below can have an impact (in varying degrees) on the operations of the AUs. Examples include:

1. Internal factors include, but are not limited to, downsizing operations, reengineering operating processes, disruption of information technology (IT) services, highly decentralized operations, providing training, and heavy reliance on contractors to perform critical functions.

2. External factors include, but not limited to, technological developments, changing needs or expectations of OMB, agency officials, the public, and new legislation and regulations.

3. Inherent factors include, but are not limited to, size of budget, nature of activities/operations, and impact external to the AU.

B. Other risk identifying considerations. To assist in identifying the AU's risks, the evaluator should consider the following questions:

1. What activities are performed in the AU?

2. What would be the consequence of not performing the activities as intended?

3. What unique risks are associated with the assessable unit (e.g., unique security considerations or the ramifications of not complying with program specific legislation or regulatory mandates)? As examples, procurement operations would be concerned with adequate competition; the payment process would be concerned with the Prompt Payment Act; or budget operations would be concerned with the accuracy of their data and conclusions and compliance with OMB Circular A-11. Where sensitive documents change hands, adequacy of security and separation of duties should be reviewed.

C. Risk ratings. After all risks have been identified for the AU, each risk should receive a prioritized ranking of high, medium, or low. The following table describes the priority impact of the risk on the assessable unit.

HIGH	The risk has been categorized as major since it has been deemed to have a considerable impact on the assessable unit's ability to meet the objective outlined. The priority on this risk is high and should be monitored closely. Any internal control weaknesses identified may result in severe impacts on the AU's performance.
MEDIUM	The risk has been categorized as average regarding impact on the assessable unit's ability to meet the objective outlined. The priority on this risk is medium and should be monitored regularly. Any internal control weaknesses identified may result in some impacts on the unit's performance.
	The risk has been categorized as minor as it appears to have little or no impact on

LOW	the assessable unit's ability to meet the objective outlined. The priority on this risk is low and monitoring can be performed on a minimal basis. Any internal control weakness identified will likely only result in minor impacts on the unit's performance. Though considered low, these risks can not be ignored because they may result in internal control deficiencies.

The focus of this rating is on the potential impact to the AU's objective if controls do not exist or are not adequate. There may be situations where a risk has a high impact but a low probability of occurrence or the reverse. In those cases, the AU point of contact should still rate the risk based on its potential impact.

040207. Determine control techniques and activities. The evaluator must document all control techniques and activities which are currently in place to mitigate risks. Control techniques and activities are implemented to ensure management's directives are followed and objectives are met based on the reduction of identified risks. Control techniques and activities occur at all levels and in all activities. Examples of control activities include, but not limited to: policies and procedures; organizational plans; managerial approvals and authorizations; verifications and reconciliation; performance reviews; security maintenance; restrictions on access to resources; segregation of duties; and documentation of transactions.

040208. Identify other objectives affected. The evaluator should consider and document any other objectives that may be impacted or overlapped by the objectives identified during the risk assessment. Based on this information, the assessable unit should be prepared to collaborate with the impacted unit within the financial management community to make sure that no control weaknesses or gaps are left unaddressed.

040209. Document and brief conclusion. The evaluator should review the control techniques and activities currently in place for each objective and risk identified. Analysis questions can include the following:

1. Do the control techniques and activities lessen or mitigate the risk to an acceptable level?

2. Do the existing control techniques and activities actually promote compliance with the objective?

3. Are control techniques and activities at the appropriate levels to ensure that objectives and risks are adequately addressed?

4. Do the control techniques and activities work, or is the action superfluous?

The risk ranking of each risk should be reflected in the control techniques and activities in place. If a control objective must be met, the control techniques and activities employed should be developed accordingly. However, absolute, or near absolute assurance is seldom required. Before control techniques are put in place to bring about absolute assurance that an objective will be met, the costs and relative benefits must be carefully considered. As control

systems approach absolute assurance, they become time-consuming and expensive. Controls should help make sure that objectives are met and risks are reduced and mitigated without substantially reducing efficiency.

Results should be briefly summarized upon completion of the evaluator's analysis of the control techniques and activities. Risks identified which, in the evaluator's opinion do not have adequate internal controls in place, should have a recommendation as to how the control technique and activity can be strengthened. The recommendation(s) should be part of a documented corrective action plan.

040210. Maintenance and review. The AU points of contact for the OCFO, Center CFOs, Mission Directorates, Mission Support Offices, NASA Competency Center, and the NSSC should maintain the completed risk assessment forms and any supporting documentation on-site to serve as a record for quality assistance visits by OQA. The supporting documentation is any materials that were used in the completion of the risk assessments (and forms). This documentation provides background support for the annual financial management internal controls certification by the Administrator under Section 2 of the Federal Managers' Financial Integrity Act. The AU points of contact should keep the Corrective Actions Plans and use them to monitor progress toward correction.

040211. Frequency. The risk assessment should be completed periodically, as directed by OQA.

040212. Develop Corrective Action Plan. The evaluator should develop a corrective action plan (CAP) in those instances where controls do not exist or are not operating effectively to address specific risks. The CAP will be fully documented on the "Financial Management Internal Control Corrective Action Plan Form" (see Appendix 3 for form and form with examples). The CAP should include the following information:

A. Assessable unit

B. Risk

C Existing control technique and activity in place

D. Recommendation

E. Implementation date (when CAP is implemented)

F. Responsible official

The CAP should be kept by the assessing organization and is required to be updated on an ongoing basis with the progress made toward correction of the recommendation.